Federal Network Security
Federal Interagency Technical Reference Architectures

Wireless Local Area Network (WLAN) Reference Architecture

Version 1.0

September 19, 2011

Department of Homeland Security
National Cyber Security Division
Federal Network Security
Network & Infrastructure Security

Revision History

Date	Version	Description	Approved By
September 19, 2011	1.0	Final Version	CS&C Acting Assistant Secretary Roberta Stempfley

Acknowledgments

This document is the product of an ongoing multi-agency collaboration to provide additional guidance for the successful implementation of Wireless Local Area Networks (WLANs) at Federal civilian agencies. Participants from several agencies have graciously volunteered their expertise; this document would not be possible without their selfless contributions.

Architecture Participants

Name	Agency
Keel Ross	Department of the Interior
John Garms	Federal Energy Regulatory Commission
Alan Smith	Health and Human Services
James K.Manzuk	Internal Revenue Service
Michael J.Varno	Internal Revenue Service
Sheila E.Frankel	National Institute of Standards and Technology
Weber Wung	Smithsonian Institution

Architecture Document Team Members

Name	Organization
Sandra Ho	Department of Homeland Security
Sean Donelan	Department of Homeland Security
Oscar Ahumada	Department of Homeland Security
Jeannette Cockrell	Department of Homeland Security
Robert L. Shaffer Jr.	MITRE Corporation
Liqun Zhang	MITRE Corporation
Mayuri Shakamuri	Sandia National Laboratories
Ryan P. Custer	Sandia National Laboratories
Robert Moore	Touchstone Consulting Group
Eric Pratsch	Touchstone Consulting Group

Table of Contents

Index of Figures

Index of Tables

1 Introduction

The use of wireless local area networks is becoming increasingly popular. This technology offers Federal agencies many potential benefits, but the architecture may be difficult to secure. The overall purpose of this Wireless Local Area Network (WLAN) Reference Architecture document is to provide Federal agencies a baseline to securely and efficiently implement a wireless architecture. This is not mandatory implementation guidance and will supplement - not repeat or replace - existing policies and standards. The document helps agencies comply with relevant Federal policies and offers best practices, which may be customized to unique Federal civilian agency requirements.

Agencies have their own business needs and may justify alternatives to the guidance in this document. When identifying alternatives to recommendations in this reference architecture, agencies must still follow existing NIST guidance for wireless networks and understand the risks and security implications of any changes.

1.1 Background

In May 2005, the United States Government Accountability Office (GAO) released a report[1] that detailed the absence of important controls to securely manage wireless networks at Federal agencies. GAO's evaluation included the 24 agencies covered by the Chief Financial Officers (CFO) Act of 1990. GAO found that many agencies did not monitor for unauthorized wireless access. Agencies lacked specific policies or procedures related to WLANs, and lacked configuration requirements for wireless assets. A few agencies did not incorporate wireless security into their training programs.

In February 2007, the National Institute of Standards and Technology (NIST) listed best practices in wireless security in Special Publication 800-97 "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i". This Special Publication assists organizations in understanding the most commonly used family of standards for WLANs, and focuses on the security enhancements introduced in the IEEE 802.11i amendment.

In June 2010,[2] the Office of Management and Budget (OMB) directed the Department of Homeland Security (DHS) to exercise primary responsibility within the Federal executive branch for the operational aspects of Federal agency cybersecurity with respect to the Federal information systems that fall within FISMA (the Federal Information Security Management Act of 2002). To support these responsibilities, DHS encourages agencies to consistently apply leading security practices and decrease agency vulnerabilities. DHS has assumed its oversight

[1] GAO 05-383, *Information Security: Federal Agencies Need to Improve Controls over Wireless Networks.*
[2] OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS).*

activities through the annual FISMA reporting process, and this architecture will serve as a foundation for future FISMA-related activities, including DHS compliance audits.

In November 2010, GAO updated its previous report[3] by examining the current state of security of wireless networks in the Federal government. Although GAO recognized progress since the previous report by identifying leading practices such as policies requiring encryption and access controls, it was apparent that many of the leading practices were not consistently applied across agencies. Gaps existed in WLAN policies and practices, many agencies used a decentralized structure for management of wireless devices, and key wireless training elements were missing from security programs. GAO recognized that agency wireless programs should be governed in accordance with FISMA reporting. GAO also recognized DHS' responsibilities for the operational aspects of WLAN security, including the development of this Reference Architecture, oversight of annual FISMA reporting, and DHS Compliance audits.

1.2 WLAN Threats

IEEE 802.11 wireless devices use radio waves to communicate, which makes the radio link vulnerable to interception, alteration, and injection of traffic. Table 1, which is taken from NIST Special Publication 800-97, lists and describes several threat categories.

Table 1: Major Threats against WLAN Security (Source: NIST SP 800-97)

Threat Category	Description
Denial of Service	Attacker prevents or prohibits the normal use or management of networks or network devices.
Eavesdropping	Attacker passively monitors network communications for data, including authentication credentials.
Man-in-the-Middle	Attacker actively intercepts the path of communications between two legitimate parties, thereby obtaining authentication credentials and data. Attacker can then masquerade as a legitimate party. In the context of a WLAN, a man-in-the-middle attack can be achieved through a *bogus* or *rogue Access Point (AP)*, which looks like an authorized AP to legitimate parties.
Masquerading	Attacker impersonates an authorized user and gains certain unauthorized privileges.
Message Modification	Attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
Message Replay	Attacker passively monitors transmissions and retransmits messages, acting as if the attacker were a legitimate user.
Traffic Analysis	Attacker passively monitors transmissions to identify communication patterns and participants.

[3] GAO 11-43, *Information Security: Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk.*

For more information on the threats associated with wireless technology, please refer to the following documents:

- Securing WLANs using 802.11i: Draft Recommended Practice. Lawrence Livermore National Laboratory for US-CERT. February 2007.
- Using Wireless Technology Securely. US-CERT: Published 2006, Updated 2008.
- NIST Special Publication 800-97 *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*
- NIST Special Publication 800-127 *Guide to Security for WiMAX Technologies*
- GAO 11-43 *Information Security: Federal Agencies Need to Improve Controls over Wireless Networks*
- US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments: Version 1.1, July 25, 2007
- US Government Wireless Local Area Network (WLAN) Client Protection Profile for Basic Robustness Environments: Version 1.1, July 25, 2007

2 Architecture Scope

This WLAN Reference Architecture focuses on 802.11 wireless networks at Federal agency buildings and campuses at the unclassified level and the devices used to access those WLANs. The main objective of this document is to help agencies securely implement a wireless infrastructure and ensure WLANs comply with Federal cybersecurity requirements. This document presents a framework for planning, procuring, deploying, and maintaining WLANs with a focus on cybersecurity. There are many other issues associated with wireless networks outside of the scope of this document; agencies must follow all appropriate Federal acquisition guidelines and requirements while implementing sound WLAN design, operational and security guidelines.

2.1 Types of Wireless Networks

The document addresses two specific types of wireless networks that have distinct business purposes: Internal WLANs and Authorized Visitor WLANs.

Table 2: Comparison of the Two Types of WLANs

	Internal WLAN	Authorized Visitor WLAN
What is the business purpose of the WLAN?	For authorized agency users to wirelessly connect to their internal networks when they are onsite at the agency.	For authorized visitors of the agency to wireless connect to the Internet, normally to VPN back to their agency.
What devices are normally used to access the WLAN?	Approved agency equipment	Visitor laptops and devices that are normally outside the control of the agency providing the WLAN.
What level of trust does the agency have with users?	Medium or higher level of trust	Low level of trust
What level of trust do users have with the connection?	Medium or higher level of trust	Low level of trust

The first type of wireless network addressed in this document is an Internal WLAN. The business purpose of this WLAN is to allow employees and contractors present at the agency's building or campus to have wireless access to internal resources and services. Users connecting to this type of WLAN will be using approved agency equipment that meets a baseline set of security controls. This network is recognized as an extension of the agency's wired network and will leverage much of the agency’s wired infrastructure for security. This WLAN sits inside the agency’s network boundary: connections to internal resources will sit “behind” Trusted Internet Connection (TIC) access points and external connections will traverse the TIC access point.[4]

The second type of wireless network addressed in this document is an Authorized Visitor WLAN.[5] The business purpose of this WLAN is to allow authorized guests of the agency to have wireless, controlled Internet access. Agencies do not have control over the devices authorized visitors use when accessing this WLAN. Generally, these users do not have a business need to access the agency’s internal network. This WLAN sits “in front of” the agency’s TIC access point and will traverse the TIC access point to connect to internal agency resources (similar to any agency external connection).

2.2 Technical Constraints and Assumptions

The architecture was developed to suit the needs of a medium-sized Federal civilian agency with 1,000 authorized users for a new, unclassified WLAN deployment. Nonetheless, the principles are applicable to agencies of all sizes and technical complexity.

The technical scope of this architecture includes authentication and access controls for WLANs. It also includes unauthorized WLAN access point device detection. Technical, Management, and Operational controls are provided for securing WLAN devices and equipment.

This document assumes that an agency’s network boundaries are secured with TIC v2.0 access points (or are leveraging a TIC-equivalent capability). For Internal WLANs, the design uses WPA2-Enterprise and EAP-TLS for wireless access directly to agency wired networks. WPA2 provides FIPS 140-2 validated encryption for wireless traffic while EAP-TLS provides mutual authentication of devices.

For Authorized Visitor WLANs, the design includes a logically separated network to provide controlled Internet access to authorized visitors. Visitors will have some formal association with the agency. Visitors are granted wireless access information through an authorized process and agree to an acceptable use policy.

[4] See the TIC Reference Architecture, Appendix A, for clarification on the “Definition of External Connection” and the distinction between internal and external connections.

[5] This reference architecture will focus on the “Official Visitor Network” – that is, individuals that are official guests of the agency that will use agency wireless devices to connect to the internet. The focus on guest networks is not meant to cover public facing networks (e.g. those found in coffee shops and airports) that the general population can access.

Items outside this document's scope include Bluetooth, Radio Frequency Identification (RFID), Worldwide Interoperability for Microwave Access (WiMAX), and telework/remote access. This reference architecture does not directly address the specific requirements for FIPS-High systems.

3 WLAN Conceptual Architecture

This reference architecture provides reasonable options for mitigating the threats mentioned in Section 1.2. Since there is no "one size fits all" solution for 802.11 wireless security, this reference architecture provides conceptual WLAN designs for deployments that are not meant to be exhaustive. Agencies should use a risk-based approach to modify this architecture in accordance with their specific needs. This architecture serves as a baseline to guide agencies to securely and efficiently implement wireless networks.

The conceptual designs presented in this document seek to mitigate the primary threats to wireless networks through the use of authentication and encryption. Authentication prevents unauthorized users and devices from accessing agency WLANs. Encryption maintains the confidentiality and integrity of traffic transmitted through agency WLANs.

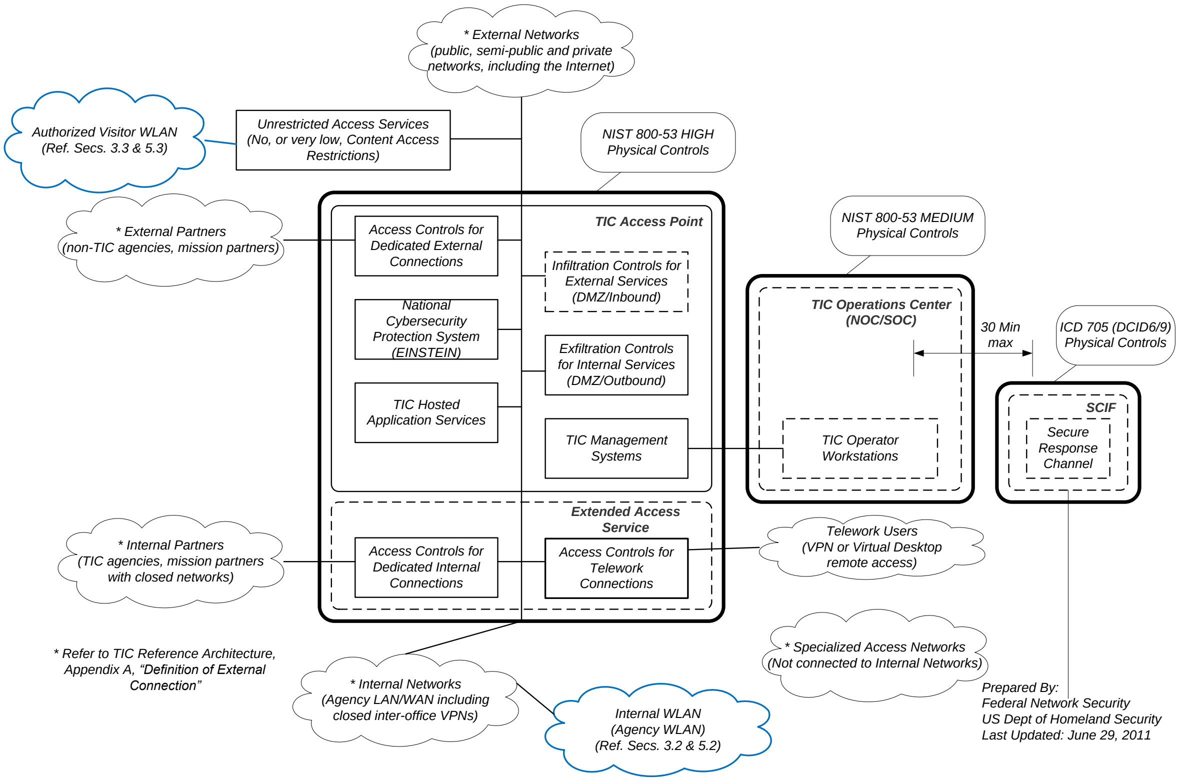
Two conceptual designs are presented in this reference architecture: one for Internal WLANs and one for Authorized Visitor WLANs. Section 3.1 reveals how each WLAN type interacts with the agency's network boundary. Section 3.2 demonstrates the conceptual design of an Internal WLAN. Section 3.3 demonstrates the conceptual design of an Authorized Visitor WLAN. Although these designs serve different purposes, they may be simultaneously deployed by agencies. With most modern enterprise wireless solutions, sufficient logical separation between the two designs can be achieved without the need to deploy physically separate infrastructures (APs, wireless controllers, WIDS/WIPS management systems, etc.).

3.1 WLANs and the Agency's Network Security Boundaries

This architecture assumes agencies are securing their network boundaries with approved TIC access points (or are leveraging a TIC-equivalent capability). An Internal WLAN extends the Internal Network of an agency by adding wireless functionality. An Authorized Visitor WLAN is logically an external network that only provides controlled access to authorized visitors.

In Figure 1, an extended version of the TIC Access Point Functional Block diagram from the TIC Reference Architecture is provided. Many of the terms and acronyms used in Figure 1 are defined in more detail in the TIC Reference Architecture, or Appendix E of this document. The two types of WLANs are shown in blue and represent where each WLAN sits in relation to the agency's network boundary (a TIC access point).

Figure 1: Extended TIC Access Point Functional Block Diagram.



* External Networks
(public, semi-public and private networks, including the Internet)
Authorized Visitor WLAN
(Ref. Secs. 3.3 & 5.3)
Unrestricted Access Services
(No, or very low, Content Access Restrictions)
NIST 800-53 HIGH
Physical Controls
* External Partners
(non-TIC agencies, mission partners)
TIC Access Point
Access Controls for Dedicated External Connections
Infiltration Controls for External Services
(DMZ/Inbound)
National Cybersecurity Protection System
(EINSTEIN)
Exfiltration Controls for Internal Services
(DMZ/Outbound)
TIC Hosted Application Services
TIC Management Systems
NIST 800-53 MEDIUM
Physical Controls
TIC Operations Center
(NOC/SOC)
30 Min
max
ICD 705 (DCID6/9)
Physical Controls
SCIF
Secure Response Channel
TIC Operator Workstations
Extended Access Service
* Internal Partners
(TIC agencies, mission partners with closed networks)
Access Controls for Dedicated Internal Connections
Access Controls for Telework Connections
Telework Users
(VPN or Virtual Desktop remote access)
* Refer to TIC Reference Architecture, Appendix A, "Definition of External Connection"
* Internal Networks
(Agency LAN/WAN including closed inter-office VPNs)
Internal WLAN
(Agency WLAN)
(Ref. Secs. 3.2 & 5.2)
* Specialized Access Networks
(Not connected to Internal Networks)
Prepared By:
Federal Network Security
US Dept of Homeland Security
Last Updated: June 29, 2011

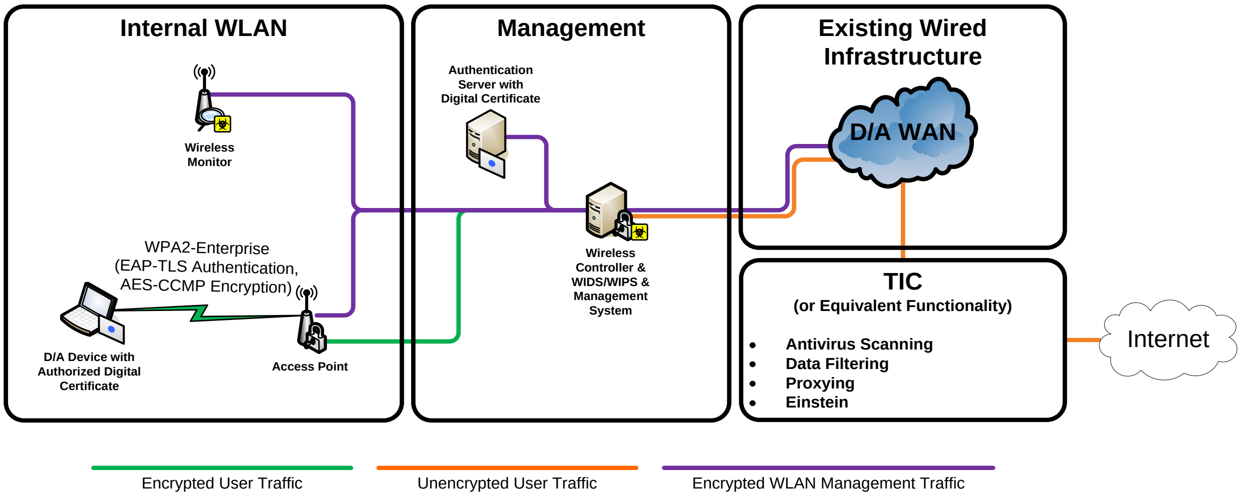
The "Internal WLAN (Agency WLAN)" cloud represents the Internal WLAN described in Section 3.2. An Internal WLAN is considered to be part of the internal network because the agency has control over the applications, software, hardware, and the assessment of security control effectiveness on the wireless network. Internal WLANs leverage WPA2-Enterprise with EAP-TLS for authentication and encryption of agency users and wireless traffic respectively. This WPA2-Enterprise solution enables WLAN users to access agency internal networks. Like all internal traffic, users of an Internal WLAN will access external networks through the TIC access point.

The "Authorized Visitor WLAN" cloud represents the authorized visitor WLAN users discussed in Section 3.3. An Authorized Visitor WLAN is considered an external network because the agency does not have full control over the applications, software, or hardware present in visitor devices. Authorized Visitor WLANs leverage WPA-2 PSK for encryption to limit access to authorized visitors. These authorized visitors are connected to a service delivery point providing controlled Internet connectivity that is outside of the agency's TIC boundary. Like all external traffic, users of an Authorized Visitor WLAN will access internal networks through the TIC access point.

3.2 Internal WLAN Logical Model

Figure 2 shows a logical representation of network components and connections to enable employees to wirelessly access agency internal network(s) using authorized devices. As stated in the GAO Report 11-43, "organizations should establish policies requiring procurement of wireless products that have been WPA2-Enterprise certified and Federal Information Processing Standards (FIPS)-validated."

Figure 2: View of Internal WLAN Components and Network Connections


Internal WLAN
Wireless Monitor
WPA2-Enterprise (EAP-TLS Authentication, AES-CCMP Encryption)
D/A Device with Authorized Digital Certificate
Access Point
Management
Authentication Server with Digital Certificate
Wireless Controller & WIDS/WIPS & Management System
Existing Wired Infrastructure
D/A WAN
TIC
(or Equivalent Functionality)
Antivirus Scanning
Data Filtering
Proxying
Einstein
Internet
Encrypted User Traffic
Unencrypted User Traffic
Encrypted WLAN Management Traffic

WPA2-Enterprise provides both authentication (via EAP-TLS) to prevent unauthorized access to the network and FIPS 140-2 compliant encryption (AES-CCMP) to ensure the confidentiality and integrity of WLAN traffic[6]. EAP-TLS is an open authentication standard that leverages a Public Key Infrastructure (PKI) to provide strong mutual authentications. This authentication and encryption scheme also enables mutual authentication between authorized devices and the wireless infrastructure. It also secures distribution of per-device wireless encryption keys. These protections mitigate both man-in-the-middle attacks and impersonation attacks against the wireless network. This conceptual model allows agencies to implement additional security measures for restricting access to the WLAN and securing user traffic.

A logically-separated management network is used for communicating with the authentication server, configuring and maintaining Access Points (APs), and transporting radio traffic received by wireless monitors to the WIDS/WIPS management system. This network is logically isolated, using a VLAN or IPSec tunnel, to prevent it from being used to access the Internet or

[6] WPA2 is backward compatible with WPA, which supports TKIP as an encryption method. TKIP is not FIPS 140-2 compliant, has known vulnerabilities, and should not be used. AES-CCMP is the preferred FIPS 140-2 compliant encryption method for WPA2 as of the writing of this document.

resources on the existing agency wired network. Traffic on this network is always encrypted to prevent an attacker from easily monitoring or injecting authentication traffic, altering the infrastructure configuration, or silencing events reported to the WIDS/WIPS management system. For similar reasons, secure management and administration methods are used when accessing the wireless controller or WIDS/WIPS management system remotely.

The high-level process is required for an authorized agency device to join the WLAN. First, the agency administrator registers the device by generating a certificate, installing it on the device, and authorizing its use for accessing the WLAN within the authentication server. Once registered, the device is authorized to access the WLAN until its digital certificate expires or its authorization is revoked. When the device associates with a WLAN access point, it is challenged to authenticate using its assigned digital certificate. The device first authenticates the WLAN infrastructure by verifying the authenticity of the digital certificate supplied by the authentication server. If the digital certificate supplied by the authentication server is genuine, an encrypted TLS tunnel is established between the device and the authentication server, through which the authentication server provides a unique AES-CCMP to the device. Using a separate encrypted channel over the wired infrastructure, the authentication server provides the AES-CCMP key to the AP. The device and AP use the unique AES-CCMP key to secure their communications, and the AP allows the device unrestricted access to the wired network.

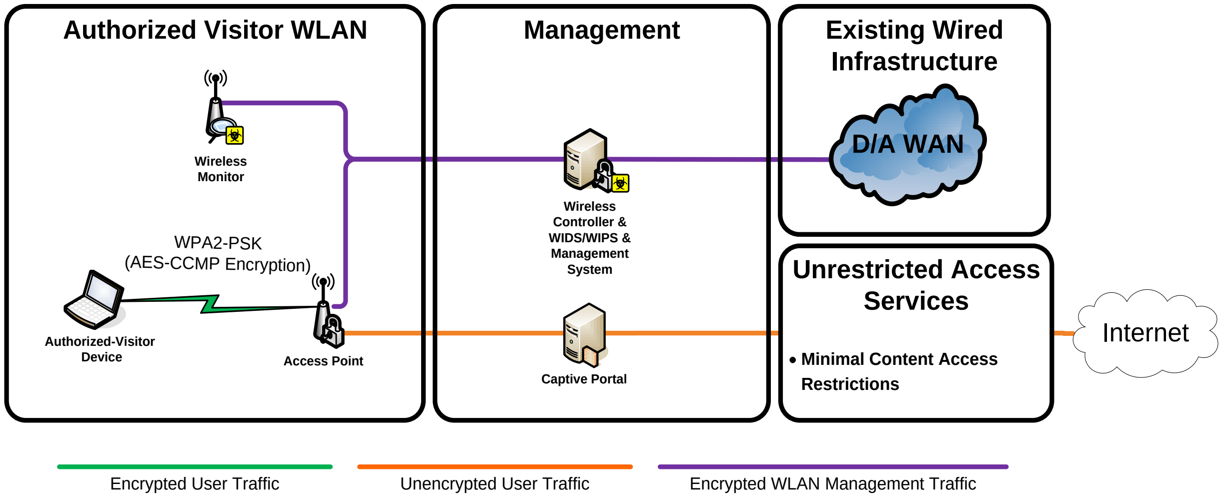
A primary benefit of this scheme is that it provides authentication and encryption that restricts access to the WLAN at the MAC layer. This reduces the opportunity for an attacker to scan devices on the wired network, mitigates the impersonated AP threat, and prevents unauthorized devices from connecting to the agency WLAN, but also comes with the downside of management overhead. Agencies must have a process to obtain or create digital certificates for each wireless device as well as the authentication servers. Agencies must also have a method to install these certificates on each of the user devices and authentication servers. If an agency has existing PKI resources this presents little additional management overhead; but if it does not then this may represent a substantial effort. The APs and client devices also require careful configuration to ensure that WPA2 encryption and EAP-TLS are properly deployed.

For detailed information on WPA2-Enterprise and EAP-TLS, please refer to sections 6 and 7 of "NIST Special Publication 800-97 *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i"* and "NIST Special Publication 800-120 *Recommendation for EAP Methods Used in Wireless Network Access Authentication*".

3.3 Authorized Visitor WLAN Logical Model

Figure 3 shows a logical representation of network components and connections to enable authorized visitors to wirelessly access the Internet using visitor-owned devices. WPA2-PSK provides AES-CCMP encryption to offer a cost-effective way to limit WLAN traffic to authorized visitors[7]. The Pre-Shared Key (PSK) is shared by all visitors, and may not protect traffic between visitors. Unlike WPA2-Enterprise, this scheme does not provide device authentication, and all devices with knowledge of the PSK share a common AES-CCMP encryption key.

Figure 3: Logical View of Authorized Visitor WLAN Components and Network Connections


Authorized Visitor WLAN
Wireless Monitor
WPA2-PSK
(AES-CCMP Encryption)
Authorized-Visitor Device
Access Point
Management
Wireless Controller & WIDS/WIPS & Management System
Captive Portal
Existing Wired Infrastructure
D/A WAN
Unrestricted Access Services
• Minimal Content Access Restrictions
Internet
Encrypted User Traffic
Unencrypted User Traffic
Encrypted WLAN Management Traffic

These protections, therefore, do not robustly mitigate the threats of man-in-the-middle and impersonation attacks against the WLAN. If desired, this conceptual model enables agencies to implement additional security measures for restricting access to the authorized visitor WLAN and securing user traffic. Password policies should be particularly stringent. It is recommended that agencies use reasonably strong passphrases to generate the PSK. Agencies are encouraged to frequently change the PSK to ensure that attackers, and formerly authorized visitors with knowledge of the PSK, cannot leverage it to maintain persistent access to the WLAN.

As in the previous design, a logically separated management network is used for configuring and maintaining APs and transporting radio traffic received by wireless monitors to the WIDS/WIPS management system. This network is logically isolated, using a VLAN or IPSec tunnel, to prevent it from being used to access resources on the existing wired network. Traffic on this network is always encrypted to prevent an attacker from easily altering the infrastructure configuration or silencing events reported to the WIDS/WIPS management system. Secure methods are used when accessing the wireless controller or WIDS/WIPS management system remotely for similar reasons.

[7] WPA2 is backward compatible with WPA, which supports TKIP as an encryption method. TKIP is not FIPS 140-2 compliant, has known vulnerabilities, and should not be used. AES-CCMP is the preferred FIPS 140-2 compliant encryption method for WPA2 as of the writing of this document.

Because agencies do not have control over the devices authorized visitors use when accessing this WLAN, authorized visitors will agree to an agency's Acceptable Use Policy (AUP) prior to using an Authorized Visitor WLAN. Agreement to the AUP is enforced through the use of a captive portal. A captive portal is used to automatically record the MAC and IP address assigned to visitor devices as they connect to the network. This record provides for device identification rather than device authentication, as a MAC address is not guaranteed to uniquely identify a single device. The time/date, IP address, MAC address, and user contact information is retained by the portal in case of problems or incidents. Creating any connection between the captive portal and any internal networks (i.e., the agency WAN or the WLAN management network) is strongly discouraged. Such connections could allow an attacker to exploit vulnerabilities in the captive portal from either the authorized visitor WLAN or Internet and leverage the connections to bypass TIC defenses protecting internal networks.

Proper wireless and wired network configuration are required to ensure that unauthorized access to internal systems and networks is not attainable from the Authorized Visitor WLAN. Access is logically restricted so that the only agency resources visible from the WLAN are the Remote Access resources. Since these resources are also accessible from the Internet, this introduces very little additional risk to internal resources. Any configuration changes made by an agency to the Authorized Visitor WLAN are well understood and documented.

The high-level process for an authorized visitor to join the WLAN follows. First, the authorized visitor obtains the passphrase used to generate the PSK from their sponsor. The visitor then uses the passphrase to join the WLAN. No WPA2 authentication is required. The first time the visitor attempts to access the Internet, the captive portal will redirect them to a web page where they can create a temporary account, including a visitor-specified username and password. The visitor must also agree to the AUP on this web page before being granted access to the Internet. At this time the captive portal records the MAC address of the wireless device, IP address assigned, and user contact information that has connected to the network. After an agency-determined period of time, such as 24-hours, the visitor will again be redirected to the captive portal to enter their username and password and agree to the terms of service. It is also important that visitor usernames and passwords be set to expire after an agency-specified period of time, preferably the duration of the visit but no longer than a year. Because WPA2-PSK is shared, it is changed on a schedule, at least annually.

Agencies may wish to use their existing processes for authorizing visitor Internet access, such as having the visitor sign a form and distributing a shared password. In these cases, it is important that the agency's policy reflects standardized processes, and that a method for disabling visitor access after the duration of the visit exists.

A primary benefit of this scheme relative to a completely unencrypted visitor WLAN is that it provides encryption that restricts access to the WLAN at the MAC layer and provides some protection of visitors' wireless communications, i.e., it acts as a "no trespassing" sign to prevent "accidental" or "unintentional" access assertions. This reduces the opportunity for an attacker to scan devices on the visitor network and provides limited mitigation of the impersonated AP.

3.4 Wireless-Free Areas

There are often special situations where an agency may wish to prohibit the use of wireless devices in some areas of campus, e.g. inside specialized labs, or near medical equipment. In such cases, the agency may wish to deploy WIDS/WIPS sensors to detect unauthorized access points or client devices that have been brought into wireless-free areas. In such cases, it is important that the WIDS/WIPS sensors operate in receive-only mode and are configured to be on a logically isolated management network. It is up to the agency to decide what countermeasures are sufficient for detecting wireless devices in wireless-free areas.

4 WLAN Security Components

The notional components of a WLAN are logically presented in Figure 2 and Figure 3 above. Each of the notional components plays a role in providing WLAN connectivity and security. Table 3 lists each component, the security features it provides, and the threats that these security features mitigate.

Table 3: WLAN Components, Security Features, and Threat Mitigations

Component	Provides	Mitigates
Common WLAN Components, Security Features and Threat Mitigations		
Access Point	WPA2-Enterprise Encryption	Eavesdropping, man-in-the-middle, denial-of-service, masquerading, message modification, message replay, and misappropriation
	Device Authentication using EAP-TLS (Authenticator)	Man-in-the-middle, masquerading, and misappropriation
Wireless Monitor	Rogue AP detection	Eavesdropping, man-in-the-middle, denial-of-service, masquerading, message modification, message replay, and misappropriation
	Unauthorized client detection	Misappropriation
	Unauthorized access attempts	Misappropriation
	Continuous monitoring of 802.11 channels	Misappropriation
	Monitoring for user devices connected to both wireless and wired agency networks	Misappropriation
Wireless Controller	Centralized management of wireless APs and User Devices	N/A
	Monitors, controls, and configures APs; enforces security policy	N/A
	WPA2-Enterprise Encryption	Eavesdropping, man-in-the-middle, denial-of-service, masquerading, message modification, message replay, and misappropriation
	Device Authentication using EAP-TLS (Authenticator)	Man-in-the-middle, masquerading, and misappropriation
WIDS/WIPS	Centralized management of Wireless Monitors, and User Devices	Unauthorized Access, rogue APs, fraudulent clients, malicious operations, ad-hoc networks.
Management System	Centralized management and configuration software	N/A

Existing Wired Infrastructure	Data Filtering	Fraud, waste, and abuse
	IDS/IPS	Intrusions from the wireless network
Internal WLAN Components, Security Features and Threat Mitigations		
Credentialed User-Device	WPA2-Enterprise Encryption	Eavesdropping, man-in-the-middle, denial-of-service, masquerading, message modification, message replay, and misappropriation
	Device authentication using EAP-TLS (Supplicant)	Man-in-the-middle, masquerading, and misappropriation
	Device certificate	Man-in-the-middle, masquerading, and misappropriation
	Two-factor user authentication	Masquerading and misappropriation
RADIUS Authentication Server	Device Authentication using EAP-TLS (EAP Server)	Man-in-the-middle, masquerading, and misappropriation
TIC	Antivirus Scanning	Propagation of malicious code
	Data Filtering	Fraud, waste, and abuse
	Proxying	Fraud, waste, and abuse
	Einstein	Intrusions
Authorized Visitor WLAN Components, Security Features and Threat Mitigations		
Guest Laptop	N/A	N/A
Captive Portal	Device Authentication	Misappropriation
	User Authentication	Misappropriation
	Mechanism to present terms of service	Misappropriation
Additional Controls	Access Controls	Fraud, Waste and Abuse
	Data Filtering	Intrusions from the wireless network
	Intrusion Detection	Intrusions from the wireless network

4.1 Access Point

The Access Point (AP) is a device that provides wireless Wi-Fi connection to wireless end-user devices and can relay data between the end-user device and other wired devices on the infrastructure. Typically the AP has a secured logical connection between itself and the Wireless Controller for managing the establishment of the end-user device connections.

In some respects, the Access Point is the first line of defense in the wireless infrastructure as it presents the wireless interface to the external user community of credentialed user devices as well as hostile threat hosts. Access Points providing the wireless interface to the Internal WLAN support WPA2-Enterprise and EAP-TLS.

4.2 Wireless Monitor

The wireless monitors provide RF monitoring of the WLAN spectrum. Wireless monitors are an important component of the WIDS/WIPS subsystem.

4.3 Wireless Controller

The Wireless Controller manages and configures the access points and wireless monitors and implements the WLAN security policies.

4.4 WIDS/WIPS

Wireless Intrusion Detection Systems and Wireless Intrusion Prevention Systems (WIDS/WIPS) are deployed to detect rogue APs and other WLAN security threats. For instance, they can detect and geo-locate a wireless Denial-of-Service attack (RF jamming or frame injection), and take countermeasure actions against the WLAN threats. They track and monitor wireless devices across the 802.11 spectrum, providing a powerful tool for network operations. WIDS/WIPS deployment is critical to the WLAN security and operation, and therefore is required by the WLAN Reference Architecture.

Because all 802.11 devices share the same frequency spectrum, an agency's WIDS/WIPS will likely detect outside APs that belong to external legitimate entities and therefore are legitimate. An agency's WIDS/WIPS will be configured not to treat these APs as rogue APs. If an agency detects that its users are connected to these external APs, the situation should be handled through user training in network security and appropriate use; and not by actions against the AP. During planning stages for a WLAN acquisition, the agency will account for these situations by addressing them in their risk plan and by defining specific requirements. WIDS/WIPS have features that enable a security specialist to monitor legitimate threats while identifying non-threats caused by these cases of overlapping WLANs.

It is important to know the limitations of WIDS/WIPS. A WIDS/WIPS can only cover a limited area due to factors such as detection range and surrounding environment. Sufficient wireless monitors are deployed at strategic positions to cover key areas within the agency perimeter. To compensate for the coverage limitation of WIDS/WIPS, agencies should integrate wireless and wired monitoring and management systems to achieve defense-in-depth network security.

In addition to the obvious use of WIDS/WIPS for security monitoring, the wireless monitoring capabilities of WIDS/WIPS can also provide operational benefits for the management of wireless networks. The wireless monitors can detect anomalous wireless network conditions such as failed or degraded APs and alert network managers to the need to take proactive response actions to resolve a WLAN outage.

4.5 Wireless Management System

The Wireless Management System is the central WLAN management system that provides configuration management and monitoring for the enterprise WLAN.

4.6 Existing Wired Infrastructure (Internal WLANs Only)

For medium-sized to large-sized WLAN installations, the wiring infrastructure requirements to interconnect the APs, Wireless Monitors with the other WLAN infrastructure components can be quite extensive. This WLAN Reference Architecture assumes that if a wired infrastructure exists in close proximity to the WLAN components, then this wired infrastructure can be leveraged to provide the necessary connectivity.

4.7 Credentialed User Device (Internal WLANs Only)

The Credentialed User Device is the end user device on the Internal WLAN that is the beneficiary receiving wireless connectivity to the WLAN. The only devices that may establish a connection on the Internal WLAN are agency-managed devices that have a device certificate that can establish wireless connectivity using WPA2-Enterprise and authenticate using EAP-TLS.

4.8 RADIUS Authentication Server (Internal WLANs Only)

The RADIUS Authentication Server (AS) provides the necessary Authentication, Authorization and Accounting (AAA) services to manage the authenticated connection of devices to the network. The function of the Authentication Service is to authenticate users or devices prior to granting network access, to authorize the appropriate network services for these users or devices and to manage the accounting for the these services. In this WLAN Reference Architecture, the RADIUS AS provides AAA support for EAP-TLS.

4.9 TIC Access Point (Internal WLANs Only)

Agencies are required to reduce and consolidate all of their external connections through approved TIC access points. WLANs will leverage existing wired network infrastructure, including TIC access points, for securing their external connections. Section 3.1 outlines where an Internal WLAN sits in relation to a TIC access point.

4.10 Authorized Visitor Laptop (Authorized Visitor WLANs Only)

The Authorized Visitor laptop is the end user device on the Authorized Visitor WLAN that is the beneficiary receiving wireless connectivity to the Authorized Visitor WLAN. Because agencies do not have control over the devices authorized visitors use when accessing this WLAN, authorized visitors will agree to an Acceptable Use Policy (AUP) prior to using the Authorized Visitor WLAN.

4.11 Captive Portal (Authorized Visitor WLANs Only)

The captive portal is used to capture all packets from the Authorized Visitor Laptop until the device has been authenticated and the user has agreed to comply with the AUP.

4.12 Additional Controls (Authorized Visitor WLANs Only)

Additional controls and protections may be required for an Authorized Visitor WLAN because it sits outside the agency’s wired network - and outside the agency’s TIC access point and its security stack.

Traffic from this network is not inspected by the National Cybersecurity Protection System, also known as EINSTEIN. An agency should define security controls for this network, such as requiring a stateful firewall that only allows normal client connections for authorized visitors including HTTP, HTTPS, DNS, and standard VPN protocols that allow Authorized Visitors to connect back to networks, such as corporate or government networks. Inbound connections should be blocked by the stateful firewall since Authorized Visitors should not have a need to set up servers on this network.

5 WLAN Security Patterns

This reference architecture describes the well-known WLAN security threats and vulnerabilities identified by the GAO report, NIST publications, industry and academic research & development, and other sources. These Security Patterns will help agencies meet federally mandated standards and industry best practices.

5.1 Taxonomy of a Security Pattern

Each security pattern includes specific security functions, capabilities, and characteristics that can be applied to a variety of IT systems with common features and policies. The same security functions may also span multiple security patterns. Security functions, with associated capabilities and characteristics in the areas of tasks, configurations, requirements and specifications, are defined as operations that are performed and functionalities that are provided to safeguard IT systems.

Figure 4: Taxonomy of a Security Pattern

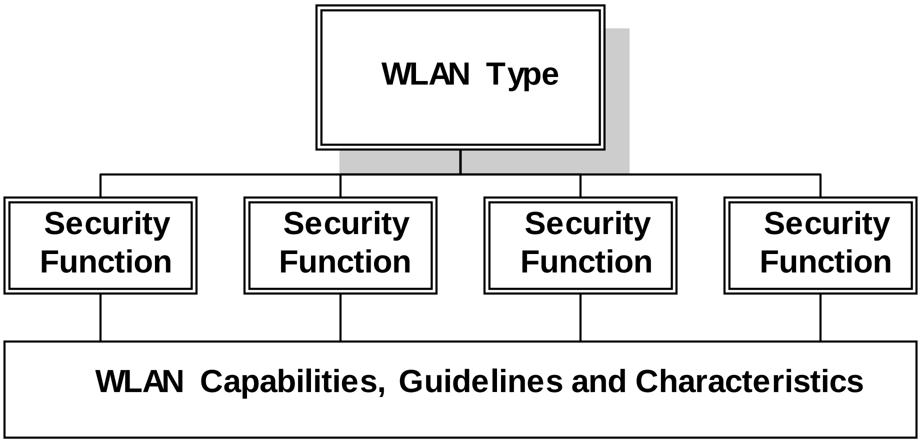


Figure 4 illustrates the Taxonomy of a Security Pattern; specifically the relationship between the WLAN Type, the Security Functions necessary to support that type of WLAN, and the resulting WLAN Capabilities attained when those Security Functions are met. The three major components of this taxonomy are:

- **WLAN Type:** A telecommunications class or pattern for data/information flow into and out of information systems, networks, or components. The architecture classifies all WLAN connections according to two connection classes: Internal WLANs, and Authorized Visitor WLANs. Each WLAN type requires a unique security pattern to build a necessary level of trust between connections.
- **Security Function:** The operations that are performed and functionalities that are provided to secure a type of WLAN. Agencies are responsible for managing these

security functions in order to meet the appropriate WLAN capabilities. Security Functions are explained in more detail in Section 6.

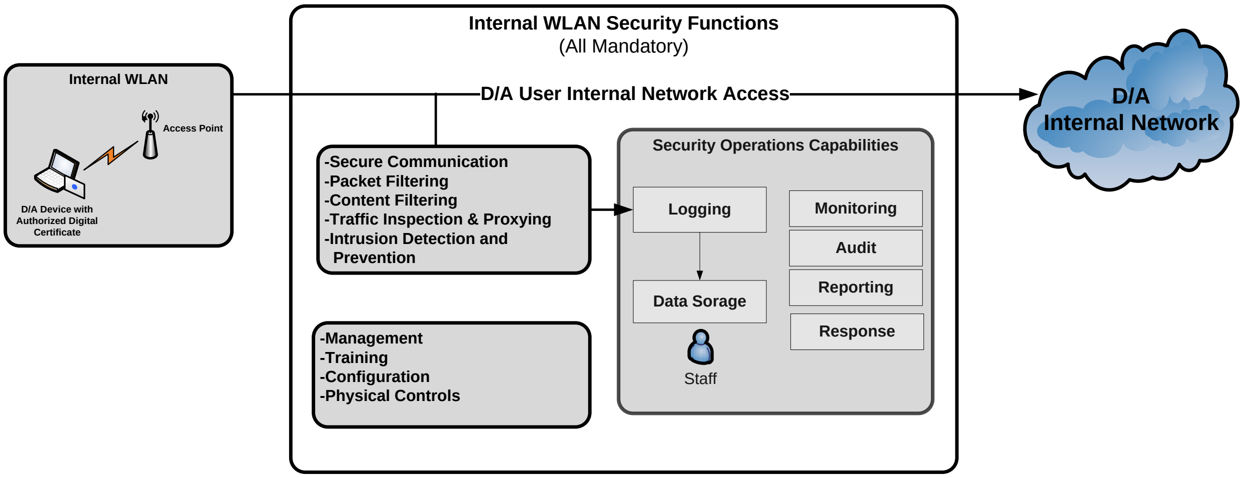
- **Capabilities:** The tasks, configurations, requirements and specifications that result from meeting specific security function(s). Each individual capability may help satisfy the execution of more than one security function, , but is categorized under a single security function in this document for simplicity. Section 7 addresses the capabilities associated with each Security Function.

5.2 Security Pattern #1: Internal WLANs

Figure 5 depicts the security pattern for an Internal WLAN. An Internal WLAN is considered to be part of the internal network because the agency has control over the applications, software, hardware, and the assessment of security control effectiveness on the wireless network.

For Internal WLANs, agencies must demonstrate that user wireless connections are secured by providing the security functions listed in Section 6.

Figure 5: Security Pattern for an Internal WLAN

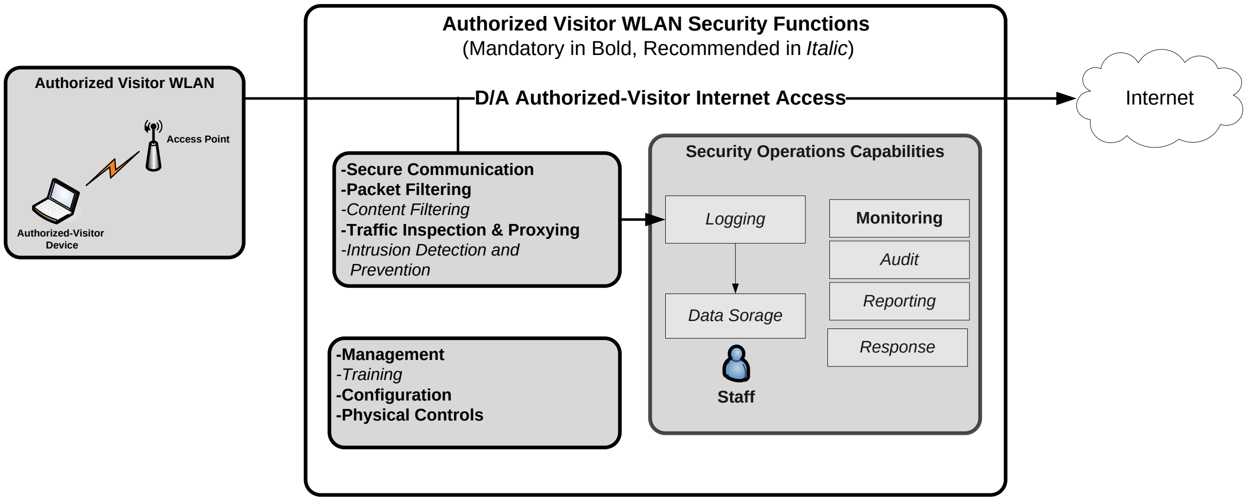


5.3 Security Pattern #2: Authorized Visitor WLANs

Figure 6 depicts the security pattern for an Authorized Visitor WLAN. An Authorized Visitor WLAN is considered an external network because the agency does not have full control over the applications, software, or hardware present in visitor devices. Agencies cannot easily assess the effectiveness of security controls on visitor devices. Furthermore, an agency may have a specific reason to believe that the network could have a substantially reduced set of security controls or an increased threat posture relative to the internal system. For instance, due to its mission and nature of operations, an agency may provide wireless services to the general public. The agency cannot apply robust security requirements to the mobile devices of the general public.

For Authorized Visitor WLANs, agencies must demonstrate that visitor wireless connections are secured by providing the security functions listed in Section 6.

Figure 6: Security Pattern for an Authorized Visitor WLAN



Authorized Visitor WLAN Security Functions
(Mandatory in Bold, Recommended in *Italic*)
Authorized Visitor WLAN
Access Point
Authorized-Visitor Device
D/A Authorized-Visitor Internet Access
Internet
-Secure Communication
-Packet Filtering
-Content Filtering
-Traffic Inspection & Proxying
-Intrusion Detection and Prevention
-Management
-Training
-Configuration
-Physical Controls
Security Operations Capabilities
Logging
Data Sorage
Staff
Monitoring
Audit
Reporting
Response

6 WLAN Security Functions

This section presents a brief description of the security functions and a summary of WLAN-related characteristics for each security function listed in Table 4. These WLAN-specific characteristics are not new requirements, but highlights of existing guidance and standards set forth in NIST publications, GAO reports, CNSS policy, Federal laws, industry standards and best-practice guidelines. General technical descriptions of security functions and their application in externally connected networks are described in great detail in the TIC Reference Architecture document.

Security functions are the building blocks for WLAN security. Unless specifically noted, all of the security functions are mandatory for Internal WLANs. For Authorized Visitor WLANs, some security functions are mandatory and some are recommended. Agencies will ensure that these security functions are incorporated into their security policies and practices.

Table 4: WLAN Security Functions

MG - Management	PF - Packet Filtering
TR - Training	CF - Content Filtering
PC - Physical Controls	LOG - Logging
AU - Authentication	TI - Traffic Inspection & Proxying
DS - Data Storage	MON - Monitoring and Auditing
CON - Configuration	RES - Response
COM - Secure Communications	REP - Reporting
IDP - Intrusion Detection and Prevention	

6.1 Management (MG)

The management security function includes the processes for assessing and managing an information processing system and the risks associated with that system. Many of the characteristics associated with management of a wired LAN apply to a WLAN. WLAN-specific characteristics include the following:

- The agency develops, documents, and implements security policies that identify which users are authorized to connect wirelessly to an organization's networks and the types of information allowed to be transmitted across wireless networks.
- The agency performs risk assessments to understand WLAN threats, the likelihood that those threats will be realized, and the potential impact of realized threats on the value of assets.
- The agency ensures resource adequacy in the following ways:
    1) Maintain a staff of cleared personnel with current credentials and adequate training to manage wireless networks.
    2) Sustain a level of funds to adequately operate and maintain wireless capabilities in accordance with applicable policy.

- A configuration baseline is established that defines the minimum requirements for compliance with policy, and ensures that wireless hardware, firmware, software, and documentation are adequate to protect the wireless information system.
- The agency designates a personnel position or organizational entity to track WLAN product vulnerabilities and wireless security trends to ensure continued secure implementation of the WLAN.

6.2 Training (TR)

The training security function addresses the necessity for network administrators to have sufficient training to administer a particular class of network, and it addresses the need for users to be educated on network-specific security issues. Training is required for every network administrator and user. WLAN administrators need sufficient training to design, operate, and maintain WLAN networks. User training on WLAN security issues provides awareness of risks associated with wireless technologies. The training security function is supported by the policies and procedures developed under the management (MG) security function.

Many of the characteristics associated with training in a wired LAN environment apply to a WLAN. WLAN-specific characteristics include the following:

- WLAN security training is part of the agency's overall security training program. Managers, technical support personnel, and users of wireless technologies are educated about the risks of WLAN technology and how to mitigate those risks before they can be authorized to operate on the wireless network.
- WLAN security training for users[8] includes WLAN security awareness, policy overview, and best practice guidelines for the following:
  - Maintaining physical control over mobile devices
  - Protecting sensitive data on mobile devices with encryption
  - Disabling wireless interfaces on mobile devices when not needed
  - Reporting lost or stolen mobile devices promptly
  - Usage policies on agency and non-agency wireless networks
- WLAN security training for managers and technical support personnel address all WLANs (Internal WLANs and Authorized Visitor WLANs) and include all user-specific security training in addition to education in the following areas:
  - Security risks associated with choosing one authentication or encryption method over another among the FIPS 140-2 approved methods
  - Wireless authentication and encryption standards such as WPA2 and EAP
  - Security requirements for the wireless network, including but not limited to security measures for data-at-rest, privacy/legal constraints, and password policy

[8] These users include all Internal WLAN users but exclude Authorized Visitor WLAN users.

- Wired LAN environment training for all personnel includes security awareness training about the risks of installing unauthorized WLAN devices.
- Individuals operating wireless scanning tools and/or analyzing results from scans are properly trained and possess a strong understanding of wireless networking—especially 802.11a/b/g/n technologies and are aware of other RF signals authorized for use within the area being scanned.

6.3 Physical Controls (PC)

The physical controls security function specifies facility, physical security, and maintenance standards that are necessary to ensure the physical security and operational resiliency of the WLAN.

Many of the characteristics associated with physical controls in a wired LAN apply to a WLAN. WLAN-specific characteristics include the following:

- A physical security plan is provided to ensure that access points, wireless monitors, and all components of the WLAN system are securely installed and can only be accessed by authorized personnel. The physical security plan also addresses response procedures for access by unauthorized personnel and requirements for AP hardware to ensure that AP configuration data is not retained when power or network connectivity is lost.
- Site Surveys are conducted to determine the proper location of APs and Wireless Monitors.

6.4 Authentication (AU)

Authentication is the process of verifying the identity of a user, process, or device. Agencies uniquely identify and authenticate network users and client devices for access to the network and resources. In a WLAN, the agency addresses the needs of both credentialed users/devices and authorized visitors/devices. All authorized visitors/devices are authenticated and only granted access to pre-defined resources such as the Internet. Only credentialed wireless users/devices that are authenticated via enterprise authentication servers are granted access to internal enterprise resources. Authentication of Authorized Visitor devices is achieved using captive portals. Captive portals, at a minimum, display AUP when an Authorized Visitor device connects to the agency's Authorized Visitor WLAN.

Many of the characteristics associated with authentication in a wired LAN apply to a WLAN. WLAN-specific characteristics include the following:

- For Internal WLANs, the agency's PKI certificate policy, certification practice statement, and related processes are revised to support the WLAN solution (e.g., revise the agency's PKI certificate policy to include the new WLAN certificates, maintenance of certificate revocation lists to include WLAN certificates, etc.).
- Records are kept for: date/time, IP address, and user contact information of authorized visitors.

- All connections to the WLAN are based on an IEEE 802.11i RSNA using IEEE 802.1X/EAP authentication.
- Only agency-issued mobile devices are allowed to access the enterprise network and resources in accordance with agency policy
- If an agency distributes Pre-Shared Keys (PSKs) rather than employing EAP methods, the keys are replaced periodically to reduce the risk that they will be compromised. The agency also ensures that no key is shared across multiple locations.

Exceptions for an Authorized Visitor WLAN include:

- There is a process in place (such as verification of visitor's valid ID, agency employee sponsoring guest access etc.) before Authorized Visitors are granted access to an Authorized Visitor WLAN.

6.5 Data Storage (DS)

Data storage is necessary to store logs collected as part of the logging (LOG) security function and data collected as part of the intrusion detection and prevention (IDP) security function. Many of the characteristics associated with data storage in a wired LAN apply to a WLAN. WLAN-specific characteristics include the following:

- Wireless security audit records are securely stored for later analysis.
- An audit record retention policy is established to meet legal and other requirements when disposing of a WLAN component.

6.6 Configuration (CON)

The configuration security function describes the appropriate logical and physical configuration settings that are necessary to deploy and maintain a secure WLAN, including its component devices. Many of the characteristics associated with configuration in a wired LAN apply to a WLAN. WLAN-specific characteristics include the following:

- WLAN configuration guidelines are developed for WLAN devices and networks, defining minimum requirements for hardware, firmware, software, and documentation. There are configuration controls to govern regular software patches and upgrades.
- For Internal WLANs, products are WPA2-Enterprise certified, FIPS validated, and support the IEEE 802.11i standard. All connections to the WLAN are based on an IEEE 802.11i RSNA using IEEE 802.1X/EAP authentication.
    - WLAN devices support the agency's chosen EAP methods.
- Vendor and default user accounts and passwords are changed before the WLAN system is put online. WLAN products are easily upgradable in software or firmware so that they can take advantage of wireless security patches and enhancements released after original delivery.
- When procuring and configuring access points (APs) for the WLAN, the following guidelines are observed:

    - The proper location of APs is based on a site survey and the desired coverage area. A complete inventory of authorized APs is maintained to support the identification of rogue APs during security audits.
    - All APs have strong, unique administrator passwords. (This is the original wording from NIST 800-97; we recommend that: "unique" password should be associated with an enterprise's wireless controller.)
    - AP configurations disable WEP and TKIP.
    - The Service Set Identifier (SSID) is changed from the vendor default setting.
    - A maximum GMK lifetime is configured on the AP, preferably not to exceed 24 hours.
    - The organization's security configuration standard is autonomously reapplied to an AP:
        - Whenever its reset function is used,
        - When an AP goes off-line, or
        - When AP is unplugged from the WLAN and is plugged back in
    - APs support authentication and encryption for administrative sessions using protections such as SSL/TLS or secure shell (SSH).
    - APs support an independent management interface to the wired infrastructure, ASs, and network management servers via a logically separated VLAN to establish an out-of-band channel for key transfer and other administrative management functions.
- When procuring and configuring Authentication Servers (ASs) for the WLAN, the following guidelines are observed:
    - Operating system and application security configuration standards are established for the agency's Authentication Servers.
    - For Internal agency WLAN, a maximum PMK lifetime is configured on the AS, preferably not to exceed eight hours. The AS is configured to use authorized EAP methods only.
- When procuring and configuring agency-issued mobile devices, the following guidelines are observed:
    - Agency-issued mobile devices use authorized EAP methods only, have enabled firewalls, have all unnecessary features disabled, and have anti-virus software with virus signatures that are updated frequently.
    - Operating system and application security configuration guidelines are established for agency-issued mobile devices.
    - Agency-issued mobile devices are configured to connect to valid ASs only. When the WLAN solution involves TLS-based EAP methods, the device's software is configured to specify valid ASs by name.
    - Ad hoc mode on agency-issued mobile devices is disabled.
    - Dual connection (wireless and wired at the same point in time) is prohibited on all mobile devices.
- When disposing of a WLAN component, all sensitive configuration information, including Pre-Shared Keys and passwords, is removed.
- Insecure and unused management protocols are disabled, and the remaining management protocols are configured for least privilege.

6.7 Secure Communications (COM)

The secure communications security function addresses the necessity of securing administratively supported communications from unauthorized access, disclosure, or modification over the air. A secure communication protocol is required to provide the appropriate confidentiality, authentication, and content integrity protection. Communications can be secured via encryption. Agencies will follow Federal encryption standards to protect WLAN data during access to information systems by users.

Many of the characteristics associated with secure communications in a wired LAN apply to a WLAN. WLAN-specific characteristics include the following:

- Sensitive data transferred on the WLAN from agency-issued mobile devices is encrypted with FIPS-140-2 validated software and/or hardware[9].
- Agency-issued mobile devices and APs support the NIST AES key wrapped with 128-bit HMAC-SHA-1 to protect transient keys during the 4-Way and Group Key Handshakes.
- Administration and network management of WLAN infrastructure equipment (i.e., APs and ASs) use strong authentication and encryption for all communications.
- APs and ASs support IPSec or equivalent protection mechanisms to establish a mutually authenticated secure communications channel between each AP and its associated ASs.

For an Authorized Visitor WLAN, there is no encryption recommended to secure the authorized visitor's communications. Authorized visitor communications traffic between the AP, captive portal interface and the Unrestricted Access Service Delivery Point is isolated from the rest of the internal network traffic using VLAN(s). Note: It is the responsibility of the authorized visitor to use mobile-user device-based security such as VPNs to secure the communications between the visitor's mobile device and external information systems. The use of such encryption is subject to the agency's policies regarding which communication ports, protocols and services are enabled on portals and firewalls.

6.8 Intrusion Detection and Prevention (IDP)

Intrusion detection is the process of monitoring network events and analyzing them for signs of potential incidents. Intrusion prevention is the process of performing intrusion detection and using automated means to attempt to stop potential incidents. In a WLAN, the network operator deploys a wireless intrusion detection system (WIDS) or Wireless Intrusion Prevention System (WIPS). WIDS detects and logs abnormal signals and physically geo-locates any suspicious devices using direction finding and triangulation algorithms. WIPS includes all of the WIDS functionality in addition to automatic functions to mitigate the harmful actions of detected

[9] It is assumed that storage of sensitive data on the Agency-issued mobile devices is done in accordance with the storage requirements for sensitive data i.e. data-at-rest.

threats. The intrusion detection and prevention security function complements the logging (LOG) and monitoring and audit (MON) security functions.

Many of the characteristics associated with intrusion detection and prevention in a wired LAN apply to a WLAN. WLAN-specific characteristics include the following:

- Deployed WIDS meets the requirements listed in the NSA publication, "Guidelines for the Development and Evaluation of IEEE 802.11 Intrusion Detection Systems (IDS)."
- WIPS meets the guidelines given in NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)," in particular those recommendations in Section 5, "Wireless IDPS," and Section 9, "IDPS Product Selection."
- Examples of event types WIDS/WIPS captures and analyzes include but are not limited to:
  - Wireless Denial of Service attacks such as RF jamming and frame injections
  - Disassociations and de-authentications that are not generated by the WLAN
  - Rogue AP (APs that have the same SSID but the MAC address is not registered)
  - Registered WLAN devices that are part of the infrastructure connecting to an AP that is not part of the WLAN infrastructure
  - Ad-hoc or bridging networks
  - Typical traffic levels for wireless devices
  - Information that existing WIDS is collecting (so that the information can be leveraged during the assessment)
- Agency security personnel maintain current knowledge of WLAN vulnerabilities such as the ones identified by severe Common Vulnerabilities and Exposures (CVE) ratings or critical vulnerabilities indicated by vendor security advisories. Some good resources for this information include:
  - The NIST National Vulnerability Database: http://web.nvd.nist.gov/view/vuln/search
  - Wireless Vulnerabilities & Exploits http://www.wve.org/entries/vulnerabilities

6.9 Packet Filtering (PF)

Packet filtering is performed by network devices such as a firewall. On a WLAN, these network devices perform traffic inspection for all communication data at the interface/boundary between the WLAN and the wired infrastructure and block traffic that is inappropriate.

Many of the characteristics associated with packet filtering in a wired LAN apply to a WLAN. WLAN-specific characteristics include the following:

- The Authorized Visitor WLAN is separated and segmented from the wired LAN, and traffic is restricted between the two networks. Authorized Visitor WLANs needs a separate security policy.

6.10 Content Filtering (CF)

Content filtering is the process of monitoring network communications at the application layer, analyzing traffic for inappropriate and suspicious content, and preventing the delivery of this content to users. Because Internal WLANs are an extension of an agency's wired LAN, there are no specific characteristics associated with content filtering of an Internal WLAN. It is assumed an agency will apply similar, if not identical, Content Filtering to a WLAN as is already applied to the wired LAN, however, content filtering requirements for Authorized Visitor Networks may be different.

6.11 Logging (LOG)

Logging is the generation, transmission, storage, analysis, and disposal of log data. The logging security function includes policy and infrastructure for the management of logs (including event, audit, error, installation, and debugging information) from operating systems, services, applications, and network devices. Additionally, logging helps to support the monitoring and audit (MON) and intrusion detection and prevention (IDP) security functions.

Many of the characteristics associated with logging in a wired LAN apply to a WLAN. WLAN-specific characteristics include the following:

- Logging captures security-relevant events, and log entries are directed to a central audit server in near real time. (Refer to WLAN event examples listed under IDP security function.) Logging may include metadata in the captive portal logs such as:
    - Session start date and time,
    - Session duration,
    - Client IP address,
    - Client MAC address,
    - Initial AP IP address
    - user ID

  Wireless security audit procedures are developed to identify the types of events that should be captured.
- If distributed WLAN systems are implemented, then centralized configuration logging and auditing are used in addition to centralized logging of all IDP events.
- Network Time Protocol (NTP) is used as the source time standard for all logs.
- All WLAN system components including APs, ASs, wireless controllers, WIDS/WIPS support and use NTP.
- Legal and privacy issues restrict the capture of authorized visitor personal data. Agencies adhere to policy and Federal laws regarding the captured log data for Authorized Visitor WLANs.

6.12 Traffic Inspection (TI) & Proxying

Traffic inspection & proxying is performed by an information system positioned between a client device and external resources (e.g., Internet). This information system is typically implemented as a proxy server. The proxy server accepts requests from the client device for resource access, analyzes and processes the requests, forwards them to the appropriate resources, and returns responses from the resources to the client device.

Many of the characteristics associated with traffic inspection in a wired LAN apply to a WLAN. WLAN-specific characteristics include the following:

- Traffic inspection & proxying is provided separately for agency Internal WLANs and Authorized Visitor WLANs, as they belong to different security trust categories.
- Traffic inspection and proxying ensures that authorized visitors have controlled access to the Internet and approved visitor network services (e.g., printers for visitors only).

6.13 Monitoring and Auditing (MON)

System monitoring and auditing are necessary to maintain situational awareness regarding the health of a network, the application of configuration changes, the detection of suspicious activities, and the implementation of corrective actions. A system audit is a periodic evaluation of security, and monitoring is an ongoing review of a system and its users. WLAN security assessments include detection of rogue APs, verification of wireless devices, configuration settings of all WLAN devices, and review of audit logs. The monitoring and auditing security function is supported by the logging (LOG) and data storage (DS) security functions, and in turn, complements the intrusion detection and prevention (IDP) security function.

Many of the characteristics associated with monitoring and auditing in a wired LAN apply to a WLAN. WLAN-specific characteristics include the following:

- Dynamic addressing
- Wireless security audit processes and procedures are developed. WLAN security assessments are performed on a regular basis (e.g., monthly or quarterly) with additional assessments at random intervals to ensure that WLAN security requirements are met. WLAN security assessments verify that the footprint, the power range, and the frequency of the WLAN devices are in agreement with the designed values. Additionally, WLAN security assessments include a WLAN device inventory check.
- Authorized wireless devices are audited periodically to ensure that they meet wireless security configuration requirements, including authentication mechanisms, data encryption, and administrative access.
- Audit logs are reviewed frequently. Auditing tool(s) can be employed to automate the review of audit data.
- The WLAN is monitored for the existence of unauthorized wireless access points and devices. If a rogue device is located, it is shut down, reconfigured, or removed completely according to agency policies and processes.
- Wireless scanning tools are capable of scanning all IEEE 802.11a/b/g/n channels, whether domestic or international. The scanning tools also support other wireless technologies (e.g., Bluetooth), capture additional radio frequencies (RF), analyze RF spectrum, plot the physical location of a device, and scan in both passive and active

modes. Individuals operating wireless scanning tools are properly trained in their use in accordance with the TR security function.

This information is used to improve security of the WLAN by:

- Detecting unauthorized devices
- Identifying operational anomalies
- Verifying that devices are agency-authorized devices only
- Identifying security configuration violations
- Locating rogue devices based on the signal strength

6.14 Response (RES)

The response security function encompasses all facets of incident response in terms of incident handling. Effective incident response requires effective processes and procedures for the six phases of incident response: preparation, identification, containment, eradication, recovery, and follow-up. The response security function is supported by the intrusion detection and prevention (IDP) security functions and directly informs the reporting (REP) security function.

Many of the characteristics associated with response in a wired LAN apply to a WLAN. WLAN-specific characteristics include the following:

- WLAN contingency plan is implemented by the agency when rogue devices are discovered.

6.15 Reporting (REP)

It is assumed an agency will apply similar, if not identical, reporting requirements to a WLAN as are already applied to the wired LAN including mandatory reporting to the United States Computer Emergency Readiness Team (US-CERT). As such, there is no capability definition defined specifically for the Reporting Security Function.

Reporting concerns specific to WLANs include:

- SSIDs of WLANs
- Locations of APs
- AP MAC addresses
- IP subnet and VLAN information
- Transmission power and range of AP
- Logs from Wireless Controllers, Captive Portals, WIDS/WIPS, and other relevant systems
- User IDs

7 Capabilities by Security Function

The capabilities listed in the table below outline the technical recommendations and guidelines to properly design, secure, manage, and operate a WLAN. The security function of each capability is indicated by its WLAN Formal ID (the first two letters in the left most column below are associated with Table 4 in Section 6). The capabilities in this table are sorted by security function.

Each capability is categorized as Critical or Recommended. Critical capabilities are baseline security features and are mandatory in order for agencies to securely implement WLANs. Recommended capabilities are best practices. Unless noted in the capability definition, each capability is applicable to both Internal WLANs and Authorized Visitor WLANs.

Table 5: Capability by Security Function

WLAN Formal ID	Capability Definition	Category Ranking
MG-1	The agency has documented and implemented comprehensive security policies for the WLAN based on current best practices for wireless networks. Policies include, but are not limited to: • Role-based access levels for WLAN • Authorized usage of WLAN • Wireless technology guidance and restrictions	Critical
MG-2	A WLAN risk assessment is performed to understand WLAN threats, the likelihood that those threats will be realized, and the potential impact of realized threats on the value of the organization's assets.	Critical
MG-3	Centralized wireless management systems are deployed unless decentralized wireless management systems are absolutely necessary to the agency's mission. If decentralized WLAN systems are implemented, then centralized configuration logging and auditing is enabled and monitored.	Critical
MG-4	For all WLAN risks identified in Table 1 of the WLAN Reference Architecture, an agency performs the following tasks, as identified in the NIST publication 800-39 Appendix E: • Risk framing • Risk assessment • Risk response • Risk monitoring	Critical
MG-5	WLAN devices and products are WPA2-Enterprise certified, FIPS-140-2-validated, and support IEEE 802.11i standard. Refer to http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm for a list of all vendors with a validated FIPS 140-2 cryptographic module.	Critical
MG-6	Requirements for a WLAN Intrusion Detection System (WIDS) are based on:	Critical

	• The technical, operational, and business goals/objectives of current system/network environment (e.g. network diagrams, OS, applications) and new the WLAN system. • The existing security protections (e.g. existing IDPS implementations, centralized logging). • Types of threats for which the WIDS provides protection • Monitoring requirements on network usage, violations of acceptable use.	
MG-7	WLAN security personnel with required skill sets are employed during design, implementation and operation of the WLAN. If an agency's personnel do not have the requisite skill sets, the services of security professionals who have the required skill sets are employed to assist during design, implementation and operation of the WLAN. Agencies ensure allocation of adequate funding to operate and maintain the WLAN.	Critical
MG-8	A fallback strategy has been established in case of WLAN authentication failure. For example, a fallback strategy to provide access to authorized user in case of forgotten password and/or lost smart card. A fallback strategy can be a technical process or may involve human process that is at least as strong as the primary authentication method.	Critical
MG-9	WLAN management establishes a WLAN configuration baseline and change control board (CCB) to formally track any modifications and maintain a proper baseline.	Critical
MG-10	Only agency-authorized mobile devices are allowed to access an Internal WLAN, wired networks and resources.	Critical
MG-11	WIDS performance is tested and evaluated before the system goes operational. WIDS evaluation includes testing of various capabilities, such as mobile sensors, fixed sensors, and sensors bundled with the APs.	Critical
MG-12	The agency has designated an individual or a group to track WLAN product vulnerabilities and wireless security trends.	Critical
TR-1	WLAN security training is part of the agency's overall security training program and is mandated on a regular basis (e.g., annually). WLAN administrators receive proper training as WLAN technologies evolve. Educate users about the risks of WLAN technology and how to mitigate those risks. WLAN security training includes WLAN security awareness, policy overview, and the following guidelines: 1) Maintaining physical control over the mobile devices (e.g., locks) 2) Protecting sensitive data on the mobile devices with FIPS approved encryption (e.g., laptops encrypted). 3) Disabling wireless interfaces on the mobile devices when not needed. 4) Reporting lost or stolen mobile devices promptly.	Critical
TR-2	WLAN security personnel operating wireless scanning tools and/or analyzing results from scans: • Possess a strong understanding of wireless networking—	Critical

	especially IEEE 802.11a/b/g/n technologies. • Are trained on the functionality and capability of the scanning tools and software to better understand the captured information and be more apt to identify potential threats or malicious activity. • Are aware of other RF signals authorized for use within the area being scanned.	
PC-1	A site survey is conducted to determine the proper location of APs and wireless monitors to monitor a desired coverage area. A physical security plan is provided to ensure that access points, wireless monitors, and all components of the WLAN system are securely installed to prevent unauthorized tampering and can only be accessed by authorized personnel.	Critical
AU-1	When WPA2 Enterprise with EPA-TLS is used, the organization's PKI certificate policy, certification practice statement, and related processes support the WLAN solution.	Critical
AU-2	Two-factor authentication is recommended by agency credentialed users and administrators for Internal WLAN connectivity.	Recommended
AU-3	EAP-TLS is used for WLAN authentication when WPA2-Enterprise is used as specified by NIST 800-120. Necessary integration has been made with PKI technology. Use of EAP-TLS will help the agency obtain the two major security objectives of EAP, which are: 1. Secure mutual authentication and authorization between a peer and the wireless access network. 2. Secure key establishment between a peer and the EAP server.	Recommended
AU-4	Connection between APs and ASs is established via IPSec/VLAN (or equivalent protection mechanism). Network management information between APs/ASs and network management servers, consoles, distribution system (e.g., enterprise wired network) is transmitted over a dedicated and logically separated management VLAN.	Critical
AU-5	When configuring WLAN authentication services to support TLS, stations connect to valid ASs only.	Critical
AU-6	When WPA2 enterprise is used, certificates on WLAN clients and servers are updated by an agency-defined time period based on agency risk assessment and Federal guidance.	Critical
DS-1	Wireless security audit processes and procedures are in place that identify the types of security relevant events that are captured and stored. Audit records are securely stored for subsequent analysis.	Critical
CON-1	All connections to an agency WLANs are based on IEEE 802.11i Robust Security Network Associations (RSNA). For WLANs using WPA2 Enterprise, only IEEE 802.1X/EAP is used for authentication.	Critical
CON-2	Operating system and application security configuration standards exist for: • Laptops and other potential STAs to account for WLAN risks. • The Authentication Servers.	Critical
CON-3	WLAN devices and products meet specifications given in NIST SP 800-97, including the following: • All stations and access points (AP) are WPA2-Enterprise certified.	Critical

	• All devices and products use FIPS-validated cryptographic modules containing FIPS-approved cryptographic algorithms, i.e., Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) uses Advanced Encryption Standard (AES), and are deployed in "FIPS mode" if required. • STAs and APs support NIST AES key wrap with 128-bit HMAC-SHA-1 to protect transient keys during the 4-Way and Group Key Handshakes. • Authentication Servers (AS) and AP support secure communication. • Devices and products support the organization's chosen EAP methods. • APs log security relevant events and forward them to a remote audit server in real time. • APs support an independent management interface to the distribution system via separate physical port or VLAN (e.g., wired network). • APs support SNMPv3 if the organization plans SNMP-based AP management. • APs support authentication and data encryption for administrative sessions. • When the WLAN solution involves TLS-based EAP methods, STA software is configured to specify valid ASs by name. • APs and ASs can support IPSec or alternative security methods to establish a mutually authenticated secure communications channel between AP and AS. • APs and ASs support Network Time Protocol (NTP). • APs terminate associations after a configurable time period. • ASs grant authorizations for a configurable time period only. • Devices and products can be upgraded easily in software or firmware.	
CON-4	Agency-authorized mobile devices have appropriate host-based defenses. Firewalls are enabled. Anti-virus software is installed and updated frequently. All unnecessary features are disabled.	Critical
CON-5	If a WLAN will be supporting unauthenticated users, such as members of the public, a network firewall is installed between each WLAN and the existing wired infrastructure.	Critical
CON-6	The SSIDs are changed from the default name. The SSID is not a common name (e.g. "wireless," "netgear," "linksys," "default" etc.).	Critical
CON-7	Multiple network connections are prohibited on all wireless client devices (e.g. connections to wired or cellular networks while connected to the WLAN).	Critical
CON-8	All insecure and unused management protocols are disabled on the APs and remaining management services are configured for least privilege. All insecure remote communications paths are disabled when configuring the WIDS, including, but not limited to: HTTP, SNMPv1, FTP, and Telnet. If they are not removed, the WIDS provides the ability to	Critical

	automatically or manually disable these paths. All alerts sent by WIDS to a system administrator, such as pager or SMS messages and emails, are properly encrypted and authenticated. WIDS has at least one secure remote communication path such as HTTPS, SSH, SFTP, SNMPv3 for: • Remote system administration and event monitoring • System updates (sensors rule sets, firmware, etc.)	
CON-9	Encryption algorithms/schemes (such as WEP, TKIP) that are not FIPS 140-2-validated are not supported by the WLAN devices.	Critical
CON-10	Group Master Key (GMK) has a maximum lifetime configured on each AP, preferably not to exceed 24 hours.	Critical
CON-11	Pairwise Master Key (PMK) has a maximum lifetime configured on the AS, preferably not to exceed eight hours.	Critical
CON-12	Ad-hoc mode is disabled on each station.	Critical
CON-13	WLAN software patches and upgrades are tested and deployed on a regular basis; the system baseline is updated as approved by the CCB.	Critical
CON-14	An inventory is maintained of all WLAN equipment , including but not limited to: • Access points • Stations and client devices • Authentication Servers • WIDS sensors The inventory information includes, but is not limited to: • MAC address(es) • Device model number • Device serial number	Critical
CON-15	When disposing of WLAN components: • All sensitive configuration information is removed, including pre-shared keys and passwords. • The component's audit records are retained as needed to meet legal or other requirements. It should be noted that simple deletion of configuration items may not result in complete destruction of the information as this is vendor and implementation specific.	Critical
CON-16	The agency's security configuration standard is re-applied whenever a WLAN device is reset.	Critical
COM-1	When VPN access is needed to access agency resources, WLAN data is encrypted with FIPS-140-2-validated software and hardware.	Critical
COM-2	Administration and network management of WLAN infrastructure equipment, such as APs and ASs, use strong authentication and encryption of all communications. All APs have strong, unique administrative passwords and all passwords are changed regularly in accordance with the	Critical

	agency's Security Policy.	
IDP-1	WIDS is able to import traffic captures from external sources such as commercial capture software, tcpdump, or network traffic analyzer. WIDS can replay the captures through the WIDS detection engine.	Recommended
IDP-2	WIDS allows administrators to selectively activate and deactivate the display of individual/unique alarms and events.	Recommended
IDP-3	WIDS supports the following: • Standardized logging and report formats • Export of event logs to industry standardized formats • Association of log entries to corresponding external references, including Common Vulnerabilities and Exposures (CVE) numbers and vendor security advisories.	Critical
IDP-4	WIDPS has multiple prevention capabilities, including but not limited to: • Enabling or disabling prevention method only for particular alert • Suppressing prevention methods for hosts on white-lists • Performing prevention actions only if a certain system is being targeted	Critical
IDP-5	WIDS is deployed to detect suspicious or unauthorized activity. Device monitoring includes recording MAC addresses of unauthorized clients and access points. WIDS security policy includes: • WIDS is up to date and current • Procedures to perform routine monitoring	Critical
IDP-6	WIDS monitors the entire 802.11 bandwidth concurrently. WIDS detects and logs the actual frame transmission frequency and not the frequency the receiver was on when the frame was captured. WIDS is able to locate all 802.11 devices and log the sensor closest to the device and preferably geo-locate the device.	Recommended
IDP-7	WIDS detects: • Signals with signal strength above the IEEE 802.11 specified levels. • Denial of service • RF interference in the frequency range allowed by 802.11a/b/g • RF jamming, frame injection • Changes in frame error rate and throughput due to active RF interference	Recommended
IDP-8	WIDS allows filtering of frames to meet the organization's privacy and legal requirements. For legal and technical reasons, the WIDS is configured to examine wireless traffic associated with the agency only.	Recommended
IDP-9	In addition to sample events described under LOG-1, WIDS detects and logs protocol anomalies including: • Violations in the 802.11a/b/g/n, 802.11i, 802.1X standards • Atypical field values, proprietary extensions, and undersized and oversized frames	Critical

IDP-10	In addition to sample events described under LOG-1, the WIDS detects and logs attack signatures (including user-defined signatures), performs stateful frame inspection and captures attacks spanning multiple frames. Additionally, the WIDS allows the administrator to create custom filters and modify/exclude existing signatures, preferably via GUI.	Critical
IDP-11	WIDS calculates normal traffic patterns; allows the administrator to manually edit the traffic; detects deviations from normal network traffic baseline; and monitors bandwidth usage, number of users, time of usage, user location, and traffic by type.	Critical
IDP-12	The WIDS tracks connection status of all clients and indicates whether a client is authorized or unauthorized. The WIDS identifies if the device is offline, its association state, and its authentication state. The system also detects and logs illegal state transitions, accumulates and analyzes profiling information over time, and provides the ability to set this time length.	Critical
IDP-13	The WIDS detects and logs: • Unauthorized clients attempting to connect to a valid agency network. • Authorized device actively communicating with an unauthorized device. • The presence of Wi-Fi bridging. • OSI Layer 2 temporal anomalies in clients and APs. This includes: • MAC spoofing and masquerading • An event logged when two sensors in physically separate (non-overlapping) locations receive frames with the same MAC address at the same time. • An event logged when a user/MAC address appears in physically distant locations in too short a time. • The presence of ad-hoc networks • A single device broadcasting beacons for an ad-hoc network • Two or more devices actively participating in an ad-hoc network • The termination of an ad-hoc network • Deviation from the security policy. This includes but is not limited to: • A device operating on the wrong channel • A violation in the broadcast SSID policy of a network • A violation in the authentication policy of a network • A violation in the encryption policy of a network • A violation in NULL SSID association policy of a network (e.g. probe requests with a broadcast SSID)	Critical
IDP-14	The WIDS maintains the status on the health of the WIDS system and generates and sends alerts when WIDS components fail to communicate.	Critical
IDP-15	All traffic between WIDS components uses FIPS-certified encryption, two-way authentication. It is recommended that WIDS components maintain a constant traffic flow to mitigate traffic analysis by non-agency	Critical

	personnel.	
IDP-16	The WIDS sensors operate in receive-mode only. Sensors do not transmit any frames when the sensor boots, no frames are transmitted during sensor operation and the WIDS system will detect, log and generate alarm if a WIDS sensor transmits. It is assumed that the WIPS sensors will transmit to mitigate an attack.	Critical
PF-1	An Authorized Visitor WLAN is separated and segmented from the agency wired LAN and traffic is restricted between them. Agency authorized visitors are not allowed to directly access an agency's wired LAN or Internal WLAN. Traffic from this network is not inspected by the National Cybersecurity Protection System, also known as Einstein, and an agency should define security controls for this network, such as requiring a stateful firewall that only allows normal client connections for authorized visitors including HTTP, HTTPS, DNS, and standard VPN protocols that allow Authorized Visitors to connect back to networks such as corporate or government networks. Inbound connections should be blocked by the stateful firewall since Authorized Visitors should not have a need to set up servers on this network.	Critical
CF-1	Content filtering for an Authorized Visitor WLAN meets the agency's security requirements for official visitors. Content filtering requirements for Authorized Visitor WLANs may be different than those applied on the agency's network.	Recommended
LOG-1	At a minimum, WIDS logs event information, such as: timestamp, event type, source of the event, the sensor or agent that detected the event, and supporting data involving the details of the event.	Critical
LOG-2	Logging is activated to capture WLAN-specific events and log entries are directed to a central monitoring and auditing server for review and audits.	Critical
LOG-3	WLAN audit logs are reviewed on an agency-defined time period based on risk assessment and Federal guidance.	Critical
TI-1	WIDS analyzes all possible frames (up to the maximum bit rate) including those with CRC or other 802.11 protocol violations. WIDS stores anomalous frames and has the ability to configure data capture parameters, perform automatic backup and store captured frames remotely. (Refer to LOG-1 for examples of event types that need to be analyzed by WIDS.)	Critical
TI-2	The WIDS identifies and logs which sensor(s) captured a frame for correlation purposes. When multiple WIDS sensors receive the same frame, the meta information (received time, received channel, signal strength, etc.) on all sensors is captured at the centralized location. The administrator sets the length of correlation time period.	Recommended
MON-1	The integrity of sensor firmware/software and management computer(s) software is checked periodically using cryptographically sound methods.	Critical
MON-2	Comprehensive WLAN security assessments are performed at regular and random intervals. Security assessments include:	Critical

	• Checking the security posture of the WLAN • Device inventory check • Identifying corrective actions necessary • Detecting unauthorized APs • Verification of STA, AP and AS configuration settings • Review of audit logs • Authentication mechanism	
MON-3	The wireless scanning tool is capable of scanning all (IEEE) 802.11a/b/g/n channels, whether domestic or international. The scanning tools supports other wireless technologies such as Bluetooth, capture additional radio frequencies (RF), analyze RF spectrum, plot physical location of the device, and is capable of scanning in both passive and active modes.	Critical
MON-4	Before a technical assessment of the WLAN is conducted, a baseline is established using factors such as: • The location and ownership of the WLAN being scanned • Security level of the data to be transmitted using WLAN	Critical
MON-5	Passive scanning is conducted regularly to supplement wireless security measures already in place, such as WIDS. During this exercise, key attributes regarding the WLAN traffic are logged. The key attributes include that should be logged include: • Service Set Identifier (SSID) • Device type • Channel • Media Access Control (MAC) address • Signal strength at various geographic locations Average number of packets being transmitted.	Critical
RES-1	The WLAN design includes the capability to terminate or quarantine WLAN operations in the event of an emergency or	Critical
RES-2	When an unauthorized device is discovered, the agency follows the policies and processes provided in the WLAN Contingency Plan. The necessary measures include: • Clear instructions on handling the rogue device • Procedures for evaluation of the rogue device activity by the security personnel	Critical

Appendix A – Glossary

Access Point (AP): An Access Point logically connects stations with a distribution system (DS), which is typically an organization's wired infrastructure. APs can also logically connect wireless stations with each other without accessing a distribution system

Authentication Server (AS): An Authentication Server provides authentication services for end-point users or stations referred to as the supplicant to an authenticator. These authentication services evaluate supplicant credentials to determine the supplicant's authorization for services provided by the authenticator

Authorized Visitor WLAN: The Authorized Visitor WLAN is a logically separated 802.11 wireless network that provides controlled Internet access to authorized visitors who have been granted permission to use the visitor WLAN. This is one of the two types of WLANs featured in the WLAN Reference Architecture.

Authorized Visitor Device: A device used to access an Authorized Visitor WLAN. Because this device is owned by a visitor, it is assumed that an agency does not own the device or have direct control over the device's configuration. Agencies do not have direct control over the device, and only can control what the device may access.

Credentials: A digital certificate issued by a trusted authority that is used in the authentication of a device.

Captive Portal: A proxy server that intercepts an attempt to connect to the Internet from Authorized Visitor Devices and redirects them to a web page where the user must agree with an Acceptable Use Policy. A username and password may also be required for access. The device is then allowed to connect to the Internet.

Internal WLAN: An Internal WLAN allows employees and contractors present at the agency's building or campus to have wireless access to internal resources and services. An Internal WLAN is recognized as an extension of the agency's wired network and leverages much of the agency's wired infrastructure for security. This is one of the two types of WLANs featured in the WLAN Reference Architecture.

VPN Concentrator: A hardware appliance that is an endpoint for encrypted VPN connections. A VPN concentrator decrypts inbound VPN traffic and encrypts outbound VPN traffic.

Wireless-Free Area: A physical volume, such as a facility with medical equipment, in which the use of wireless devices is prohibited.

Wireless Intrusion Detection System (WIDS): A WIDS detects threats or attacks to a wireless network infrastructure. A WIDS differs from a Network Intrusion Detection System (Network IDS or NIDS) in that it monitors attacks that leverage wireless protocols.

Wireless IDPS Sensor: A Wireless Intrusion Detection and Prevention System (IDPS) Sensor is a device used by a Wireless IDPS to monitor a wireless network. Wireless IDPS Sensors can also be referred to as Wireless Monitors or Access Monitors.

Wireless Intrusion Prevention System (WIPS): A WIPS includes all of the WIDS functionality in addition to automatic functions to mitigate the harmful actions of detected threats.

Wireless IDS Management System – A server that provide centralized management and configuration capabilities for the WIDS and all WIDPS sensors.

Appendix B – Acronyms

AES - Advanced Encryption Standard
AES-CCMP - Advanced Encryption Standard-CCM Mode Protocol
AP - Access Point
ASLEAP – Automated hacker tool for gaining access to network protected by LEAP
AS - Authentication Server
CCB - Change Control Board
CFO - Chief Financial Officers
CNSSP - Committee on National Security Systems Publication
CVE - Common Vulnerabilities and Exposures
CRC – Cyclic Redundancy Check
DHS – Department of Homeland Security
DISASSOC – Disassociation as in a disassociation Denial of Service Flood attack
EAP-TLS - Extensible Authentication Protocol-Transport Layer Security
FIPS - Federal Information Processing Standards
FTP – File Transfer Protocol
GAO - Government Accountability Office
GMK - Group Master Key
GUI – Graphic User Interface
GuestNet – Guest WLAN Zone
HMAC-SHA-1 - Hash-based Message Authentication Code for Secure Hash Code
HTTP – HyperText Transfer Protocol
HTTPS - Hypertext Transfer Protocol Secure
ICMP - Internet Control Message Protocol
IDPS - Intrusion Detection and Prevention System
IEEE - Institute of Electrical and Electronics Engineers
IPSec - Internet Protocol Security
MAC - Media Access Control
MD5 - Message-Digest algorithm 5
NIST - National Institute of Standards and Technology
NSA – National Security Agency
NTP - Network Time Protocol
OSI - Open Systems Interconnection
PMK - Pairwise Master Key
PSK – Pre-Shared Key
RF - Radio Frequency
RFID - Radio Frequency Identification
RSN – Robust Secure Network
RSNA - Robust Security Network Associations
SFTP – Secure File Transfer Protocol
SHA-1 – Secure Hash Algorithm
SNMP – Simple Network Management Protocol
SP – Special Publication
SSID - Service Set Identifier
STA – Station in IEEE 802.11 terminology
TCP - Transmission Control Protocol
TIC - Trusted Internet Connection
TKIP - Temporal Key Integrity Protocol
TLS – Transport Layer Security
UDP - User Datagram Protocol
US-CERT – DHS's United States Computer Emergency Readiness Team
VLAN - Virtual LAN
VPN – Virtual Private Network
WEP - Wired Equivalent Privacy
Wi-Fi – Trademark of Wi-Fi Alliance
WIDS - Wireless Intrusion Detection System
WIDPS - Wireless Intrusion Detection and Prevention Systems
WIPS – Wireless Intrusion Prevention System
WPA2 - WI-FI Protected Access 2
WLAN - Wireless Local Area Network

Appendix C – References

STUDIES

U.S. Government Accountability Office (GAO), GAO-11-43, *Information Security: Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk,* November 30, 2010.

U.S. Government Accountability Office (GAO), GAO-05-383, *Information Security: Federal Agencies Need to Improve Controls over Wireless Networks,* May 17, 2005.

GUIDELINES

Committee on National Security Systems No. 17: Policy on Wireless Communications: Protecting National Security Information, May 2010

National Institute of Standards and Technology Special Publication 800-48, Revision 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks, July 2008.

National Institute of Standards and Technology Special Publication 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009.

National Institute of Standards and Technology Special Publication 800-53A, Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans, June 2010.

National Institute of Standards and Technology Special Publication 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS), February 2007.

National Institute of Standards and Technology Special Publication 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, February 2007.

National Security Agency's Guidelines for the Development and Evaluation of IEEE 802.11 Intrusion Detection Systems (IDS), November 1, 2005

National Security Agency's Recommended 802.11 Wireless Local Area Network Architecture, September 23, 2005

US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments: Version 1.1, July 25, 2007

US Government Wireless Local Area Network (WLAN) Client Protection Profile for Basic Robustness Environments: Version 1.1, July 25, 2007